Orwellian Nightmare Down Under? by Stewart Taggart

Story location: http://www.wired.com/news/politics/0,1283,32853,00.html

03:00 AM Dec. 04, 1999 PT

SYDNEY, Australia -- Any data seem different on your computer today?

If you're in Australia, the government has the ability to modify your files. Its cyber spooks have been given legal power not only to monitor private computers around the country, but to change the data they contain.

The new powers are contained in a bill passed by Australia's parliament late last month (the Australian Security Intelligence Organization Legislation Amendment 1999). They now await only the largely ceremonial assent of Australia's governor general before becoming law.

"These are really untested waters," says Chris Connolly, a vocal Australian privacy advocate. "I don't think there's any example anywhere else in the world that's comparable."

Under the new law, Australia's attorney general can authorize legal hacking into private computer systems, as well as copying or altering data, as long as he has reasonable cause to believe it's relevant to a "security matter."

The keyboard spies will come from the Australian Security Intelligence Organization (ASIO), Australia's equivalent of the Central Intelligence Agency. Catherine Fitzpatrick, spokeswoman for Attorney General Daryl Williams, said the law merely "modernizes" an existing 1979 statute that previously governed ASIO, and sorely needed updating.

"This just brings ASIO's powers in line with new technologies," she said. "It doesn't give them increased powers at all."

For example, the new law bars sleuths from introducing viruses or interfering with data used for lawful purposes on targeted computers, she said. In addition, the bill limits the power to alter data on a computer to concealing surveillance, she said.

While all this is true, the bill also specifically authorizes -- among other things -- anything that's "reasonably incidental." And it's broad wording like this -- as well as the weak oversight of the nation's cyber spies -- that have opponents aghast.

"I hate to use the word 'Orwellian,' but I can't think of anything better to

describe this," said Greg Taylor, vice chairman of Electronic Frontiers Australia.

"This is another stop down the path of legalized surveillance of all information by authorities," he said.

Taylor believes the new law could be especially damaging to people's faith in encrypted communications, because government hackers could potentially lift encryption keys from individual computers.

"This bill seems to get around the problems that strong cryptography presents law enforcement," Taylor said. "Now, they can attack the problem at the source -- the originating computer -- before the data even gets encrypted."

In addition, the new law could introduce tricky new issues into legal cases, he said. "It opens to question all computer evidence if there's been the potential for legalized tampering of it. Computer evidence already poses problems of validation, and that's before you even open up these legal avenues of tampering."

Connolly, as director of Australia's Financial Services Consumer Policy Center and national coordinator of the Campaign for Fair Privacy Laws, spoke out against the proposed legislation in a parliamentary submission earlier this year.

"Australia doesn't really need an intelligence agency with dictatorial powers," he said. "People here largely trust the federal police to deal with most matters, and the police are subject to more controls and supervision by judges than ASIO is."

He believes the government hastily pushed the bill through parliament using, among other things, national nervousness about the approaching Sydney Olympics to convince parliamentarians to go along. He thinks ASIO's expanded powers clearly go too far, and were sought by an agency seeking a new role after the Cold War.

To Brian Greig, a West Australian senator from the populist Democrats Party -- which voted against the bill -- the law now tilts the balance of power between the individual and government too far in favor of government.

"If we're going to expand ASIO's surveillance powers, we should have expanded equally the rights and liberties of individuals to be protected from that," he said. "My suspicion is that citizens of other countries wouldn't have been so apathetic about an issue like this."

As Australia's fourth largest political party, the Democrats could only voice concern about the proposed law. Both the ruling Liberal-National party coalition and the opposition Labor Party both voted to pass the measure.

Under the new system, a citizen's most likely recourse if he feels improperly snooped would be to complain to the attorney general -- who authorized the snooping in the first place, or to the inspector general of intelligence and security, a government watchdog that conducts periodic reviews of ASIO's activities, Connolly said. Neither of which is likely to pursue an aggressive, impartial investigation, Connolly believes. So, if the law's a done deal -- what now?

Connolly suggests it's up to individuals and companies in Australia to take additional measures to protect confidential information if they're worried about government hackers. He suggests seeking out better encryption, as well as software that can detect computer intrusions.

However, if government now has legal power to change computer data, it can legally tamper with intrusion detection software, erasing records of its visits, he said.

To Paul Budde, a Sydney-based independent telecommunications analyst, the new law sends the wrong message.

"If the government is allowed to be the biggest hacker in town, it really undermines computer security rather than enhances it," he said. "How can they now criticize 16-year-old kids who break into computer systems for fun if the government's doing it, too?"